

LIBRARY OF THE
UNIVERSITY OF ILLINOIS
AT URBANA-CHAMPAIGN

510.84

Il63c

no. III-120



ENGINEERING

AUG 5 1976

The person charging this material is responsible for its return to the library from which it was withdrawn on or before the **Latest Date** stamped below.

Theft, mutilation, and underlining of books are reasons for disciplinary action and may result in dismissal from the University.

UNIVERSITY OF ILLINOIS LIBRARY AT URBANA-CHAMPAIGN

ENGINEERING

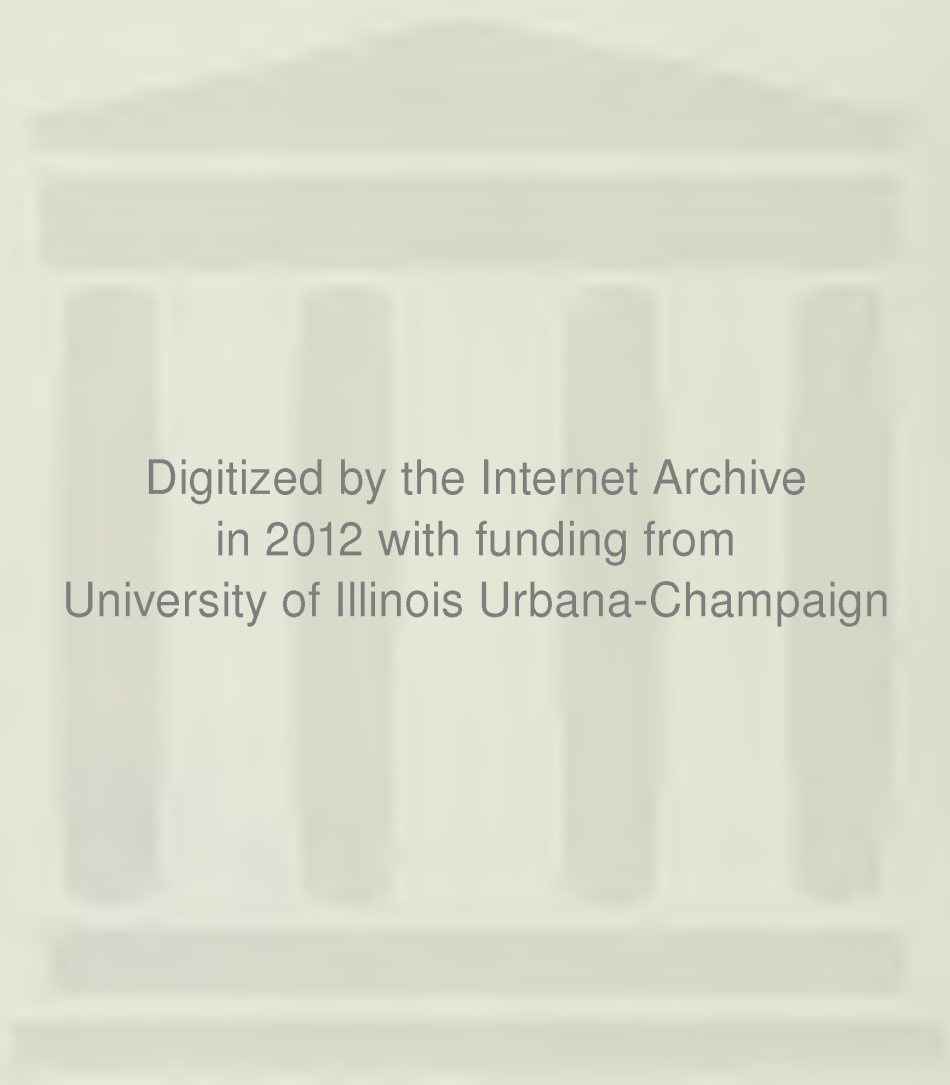
CONFERENCE ROOM

JUL 2 1979

JUN 11 1991

FEB 27 1991

MAR 05 1991



Digitized by the Internet Archive
in 2012 with funding from
University of Illinois Urbana-Champaign

Engin.

ENGINEERING LIBRARY
UNIVERSITY OF ILLINOIS
URBANA, ILLINOIS

CONFERENCE ROOM

Center for Advanced Computation

UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN
URBANA, ILLINOIS 61801

CAC Document No. 120

THE LEGAL PROTECTION OF COMPUTER SOFTWARE

by

John T. Soma*
and
Richard Michael Fischl**

October 1974

The Library of the

MAY 5 1976

University of Illinois
→ Urbana-Champaign

THE LEGAL PROTECTION OF COMPUTER SOFTWARE

by

John T. Soma* and Richard Michael Fischl**

October 1974

Center for Advanced Computation
University of Illinois at Urbana-Champaign
Urbana, Illinois 61801

* Mr. Soma received his J.D. from the University of Illinois, College of Law in 1973 and is a member of the Illinois Bar. He received his M.A. in Economics from the University of Illinois in 1973, and presently he is a candidate for a Ph.D. in Economics at the University of Illinois, and a Research Assistant at the Center for Advanced Computation, Urbana, Illinois.

** Mr. Fischl has studied political science at the University of Illinois. He has been accepted by the University of Illinois, College of Law, and will be attending the College of Law beginning in the Fall of 1975.

ABSTRACT

Software technology has outgrown the legal development of software protection. This document examines the legal protection of software through the use of patent, copyright, and trade secret law. Each of these methods offers a viable alternative, but each suffers from major weaknesses. The unique legal problems encountered by a university in software development are then examined, followed by a discussion of Federal Government software procurement policies. Finally, the legal interaction between private and university software developers and the Federal Government is briefly examined.

TABLE OF CONTENTS

	Page
PATENT PROTECTION	3
<u>Gottschalk v. Benson</u>	4
COPYRIGHT PROTECTION	6
<u>Telex v. IBM</u>	7
TRADE SECRET PROTECTION	8
Federal Preemption of State Trade Secret Law	11
Software and Trade Secrets	14
Scope of Protection	16
Criminal and Non-Criminal Remedies Under Trade Secret Law. .	18
THE UNIVERSITY ENVIRONMENT AND PROTECTION OF SOFTWARE	20
Academic Freedom	23
GOVERNMENT PROCUREMENT OF SOFTWARE	24
Patents Rights and Rights in Data Clauses	25
Software Revision to ASPR's.	27
CONCLUSION	28
NOTES	30

THE LEGAL PROTECTION OF COMPUTER SOFTWARE[†]

The computer software industry is one of the most dynamic growth industries in the United States. In the 1950's and 1960's the emphasis was on hardware development, but in recent years the emphasis has shifted to software development.^[1] As an example of this shift, after the hardware was developed for the IBM 360 series, it took five years to develop the supporting software.^[2] The industry is highly innovative and has low barriers to entry.^[3] The legal structure surrounding the software industry has not, however, kept pace with the technological changes occurring within the industry. Although there is voluminous material on the legal protection of software, no definitive legal principles have emerged concerning the procedures used to protect software.^[4]

Rapid software development, however, is essential for the continued growth of the computer industry. Today software packages are commonly sold for thousands of dollars. In addition, there are now large numbers of identical computers available upon which these

[†] The authors gratefully acknowledge the assistance and support given by Professor Hugh Folk, Director, Center for Advanced Computation. In addition, we wish to thank Professor Peter Maggs, College of Law, University of Illinois, for reading an earlier draft of this document, Dr. Donald Bitzer, Director, Computer-based Education Research Laboratory, University of Illinois, for many helpful comments and suggestions, Barry Sufrin for several ideas on the academic freedom issue, and Carol Boast, Assistant Law Librarian, and Madhavarao Balachandran, Assistant Commerce Librarian for their tireless support in the research of this document. We also wish to thank Frieda Anderson, Center for Advanced Computation, for providing the ever necessary administrative coordination in the preparation of this document. Any errors remaining, however, are those of the authors.

software packages can be used. Large social gains exist if these software packages can be used on all machines rather than having a similar software package independently developed for each computer. Consequently, some type of legal mechanism is essential to provide software developers with a means to protect their intellectual products. Once appropriate legal protection is provided, the developers of software will be willing to sell their products, and thus wasteful duplication of effort can be avoided. By providing a viable method to protect software, public policy will therefore foster the commercial development of software. The social gains from such protection are greater today than in the 1950's and 1960's due to the recent shift in emphasis from hardware to software development.

This document has been prepared to review the present legal status of software protection. Rather than investigating a few areas in great detail, this document will overview the entire area of software protection. Appropriate footnotes will be used to guide the reader to additional materials on each topic. A major patent revision bill is currently before Congress, and numerous legal doctrines are still in the developmental stage. Therefore, the entire legal area of software protection can be expected to remain in a state of flux for the foreseeable future.

The remainder of this document will first examine the legal protection of software through the use of patent, copyright, and trade secret law. Each of these methods offers a viable alternative, but each suffers from major weaknesses. The unique legal problems encountered by a university in software development will then be examined, followed by a discussion of Federal Government software procurement policies. Finally, the legal interaction between private and university software developers and the Federal Government will be briefly examined.

PATENT PROTECTION

Although hardware is clearly patentable under existing patent statutes,^[5] software does not conveniently fall into any of the present statutory classifications of patentable material. As a result of this ambiguity over software patentability, several test cases have attempted to define the limits of software patentability. Patent protection is commonly accepted as the strongest form of software protection, and thus several proposals are currently before Congress which would allow patenting of software.^[6]

The status of the various patent law revisions before Congress is constantly changing. Consequently, this area will not be examined due to the speculative nature of any inquiry at the present time. Instead, the present focus will be on the current legal interpretation of this existing patent law with regard to software patentability.

In several early cases, the Supreme Court held that a newly discovered scientific truth or mathematical expression could not be patented, but that "a novel and useful structure created with the aid of knowledge of scientific truth may be."^[7] From this line of cases, and others related to the field of electronics,^[8] the Court developed the mental steps doctrine.^[9] In brief, the mental steps doctrine means that if an idea can be totally carried out by the human mind without the aid of a mechanical device, then the idea is unpatentable. Applied to computer programs, the result is devastating because most software can at least theoretically be performed by the human mind. The time required for such operations, however, would be measured in years as compared to seconds with the aid of a computer.

Through a series of cases, the Court of Customs and Patent Appeals (hereinafter CCPA) attempted to distinguish computer programs which provided some physical change on materials from programs which did not physically affect materials.^[10] Based on this distinction,

the CCPA distinguished computer programs performing some physical act on materials from the mental steps doctrine and upheld several patents on computer programs. While the Patent Office and CCPA were distinguishing types of computer programs, the President's Commission on the Patent System concluded that the Patent Office lacked adequate methods and facilities for classifying computer programs, and thus recommended against a patent policy which would allow the patentability of computer software.^[11] Due to the diversity of opinions and the resulting ambiguity over software patentability, the legal status of patenting software remained unclear.

Gottschalk v. Benson

In 1972, the Supreme Court attempted to clarify this confused situation by deciding Gottschalk v. Benson.^[12] Gary Benson and Arthur Talbot filed an application with the Patent Office in 1963 seeking a patent on a method of converting binary coded decimal (BCD) numerals into pure binary numerals through the use of a mathematical algorithm. Although this process could be performed mentally with the aid of pen and pencil, the algorithm enabled one to program a computer to do the same conversion with large savings in manpower and time. The Patent Office refused to issue the patent on the ground that the subject matter of the invention was not within any of the statutory classes of patentable inventions.^[13] The Patent Office reasoned that the application was within the mental steps doctrine and thus outside of the statutory class of patentable material. On appeal, the CCPA reversed the Patent Office decision and held that the patent application claims were within the statutory classification of patentable inventions and thus patentable as a process under the existing patent statutes.^[14]

Writing for a unanimous court with three justices abstaining, Justice Douglas held that the invention was not patentable under the existing patent laws. Based on the settled principle that ideas were

not patentable, the Court reasoned that granting a patent for converting BCD to binary numerals with the aid of a digital computer would in effect be a patent on the algorithm embodied in the computer program since the use of the algorithm on a digital computer would be the only practical method of implementation. The opinion did not mention the earlier cases developed by the CCPA which had attempted to distinguish patents issued for computer programs from the mental steps doctrine. Consequently, the validity of this line of cases is questionable. Justice Douglas, however, stressed that the opinion was limited only to invalidating the patenting of a mathematical algorithm and not the invalidation of all computer programs.

One possible interpretation of Gottschalk is that mathematical algorithms are not constitutionally patentable even if Congress were to amend the patent laws to include them in the statutory classification of patentable material.^[15] Then as a corollary, programs which use computers to solve mathematical problems are not currently patentable due to the present patent law. Thus, impliedly, the existing laws could be amended to include software as a statutory class of patentable material. The result of Gottschalk, however, is that at present the status of software patentability is very ambiguous. Another interpretation of Gottschalk is to read the opinion narrowly and conclude that only the patenting of mathematical algorithms in computer programs is prohibited.

The CCPA is still validating patents for computer programs which adequately describe the program and which do not relate to a purely mathematical algorithm.^[16] The legal support for issuance of these patents, however, is based on the pre-Gottschalk case law distinguishing computer programs from the mental steps doctrine.^[17] The true test of these cases will be a patent infringement suit. The overall likelihood of a patent holder having his patent validated in a patent infringement suit is presently low.

On the practical side, a strong deterrent exists against the use of patents to protect software. The minimum cost of obtaining a patent is approximately one thousand dollars with many patent applications being considerably higher. The average cost for software patents may be considerably higher due to their controversial nature. In addition, the gestation period for a patent application averages three years, and thus if a patent is finally disapproved, the developer of a program will be left in the same position he was before beginning the patent application procedure. Finally, as previously stated, many patents are invalidated in infringement suits. With the current high standards of disclosure, once a patent is declared invalid in an infringement suit, its contents are known, and thus trade secret protection is no longer available. The net result of these difficulties is that the choice of patent protection for software is not particularly inviting.^[18]

COPYRIGHT PROTECTION

The difference between patent and copyright protection is that a patent holder acquires exclusive right to the invention even if another individual later, but independently, discovers the same idea.^[19] A copyright, however, only protects one from the mere copying of the idea or work. For example, if a computer program were patented, no one could use the same program even if they independently discovered the program. A copyright, on the other hand, would only prevent others from copying the exact program. Consequently, if an individual could prove that he independently developed the program, then the individual could freely use the program which he independently developed.^[20]

There are two types of copyright protection. One based on common law and the other based on federal statutes.^[21] While an author is preparing his work and up to the time the work is published, the author is protected under state common law copyright. This means

that the author is protected from unauthorized copying, publishing, vending, performing, and recording of his work.^[22] Under present law, until the author permits publication, this common law protection exists forever.^[23] Once the author decides to publish the work, one of two alternatives will occur.^[24] First, the author can publish the work without any copyright notice on the work. If this happens, the work is considered to have been donated to the public. On the other hand, if all copies of the work which are authorized by the author are properly designated as copyrighted material, then the author is protected under federal copyright statutes. The duration of the federal copyright protection is 56 years if the copyright is properly renewed after 28 years.^[25] Under both common law copyright and statutory copyrights, the author can sue for damages for illegal copying of his work.^[26] Damages are based on either actual damages which he has suffered, or the profits which the copier received from the unauthorized copying.

In 1965, the Copyright Office issued Circular 31D which outlined the three basic rules for current registration of computer programs.^[27] The first rule is that the individual applying for the copyright must be the original author. Next, all copies of the program must be published with the normal copyright designation. Finally, copies of the program must be deposited with the Copyright Office, and if the program is in machine language, copies of the program both in machine language and in a high level language must be deposited with the Copyright Office.^[28]

Telex v. IBM

On the practical side, one method to prevent copyright infringement is to insert meaningless statements into the program.^[29] If the alleged infringer literally copied the program, these meaningless statements will appear, and thus sufficient evidence will be available to prove infringement. If the program is extremely long,

the proof of availability of the program to the defendant and complete identity will also be sufficient evidence to prove copyright infringement. In Telex v. IBM ^[30] one of the counter claims by IBM against Telex was for copyright infringement of IBM's Fast Running Interpreter Enabling Natural Diagnostics (FRIEND) program. The Telex court accepted as sufficient evidence that out of the entire program only a few minor deviations existed between the IBM original and Telex's version. In addition, IBM was able to prove that Telex personnel had access to the IBM program.

In Walt Disney v. Alaska Television Co., ^[31] the court held that copyright infringement had occurred when the defendant copied a television show and transported it to Alaska on magnetic tape. The mere copying onto magnetic tape was considered the critical element, not the rebroadcast of the performance. By analogy, one can reason that the copying of a computer program which is on magnetic tape is also a copyright violation. Translations of copyrighted material are also prohibited, and thus the conversion of a copyright program from one language to another through a compiler should also constitute copyright infringement. ^[32]

IBM Corporation has favored copyright protection, and Elmer Galbi, Senior Patent Attorney for IBM, has proposed a revision to the Copyright Act which includes a provision allowing the copyrighting of computer software. The future of copyright protection of software is still uncertain. ^[33] If the counterclaim in Telex v. IBM is appealed by Telex, the Telex case will be the first software copyright case decided by a court of appeals. ^[34]

TRADE SECRET PROTECTION

A viable third alternative for many firms is the use of trade secret law to protect software. Just as common law copyright law originates in the common law of each state, the origin of trade secret law can also be found in the common law of each state. Although

the scope and vitality of state trade secret law varies from state to state, ^[35] the Restatement of Torts offers a useful definition:

A trade secret may consist of any formula, device, or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it.^[36]

In Illinois, a trade secret is judicially defined as "a secret plan or process, tool, mechanism or compound known only to its owner and those of his employees to whom it is necessary to confide it."^[37]

Judicial recognition of trade secret law has a long history. Speaking for the Court in Board of Trade of Chicago v. Christie Grain and Stock Co., Justice Holmes recognized trade secret law when he stated that "the plaintiff has the right to keep the work which it has done, or paid for doing, to itself. The fact that others might do similar work, if they might, does not authorize them to steal plaintiff's."^[38] In a later case, however, Justice Holmes pointed out that it is not the subject matter per se which gains for itself the status of trade secret, but rather "the primary fact that the law makes some requirements of good faith ... The property may be denied, but the confidence cannot be."^[39]

In order to find sanctuary in the law of trade secrets, state courts have held that a trade secret must meet four major tests: 1) appropriateness of subject matter, 2) secrecy, 3) novelty, and 4) economic value.^[40] Appropriateness of subject matter has three broad subcategories of protectable information: 1) patentable and unpatentable inventions along with know-how associated with these inventions (e.g., secret processes, patterns, compounds), 2) abstract ideas of a commercial or industrial nature (e.g., advertising plans, schemes for media presentation), and 3) other sorts of information which are not novel, but which are of value to the owner (e.g., customer lists, discount codes, supply sources).^[41]

The second requirement of secrecy is rather vague and has at least two interpretations: internal and external secrecy.^[42] The distinction between internal and external secrecy is basically one between in-house secrecy (which involves the steps taken by the owner of the secret to prevent its disclosure by those in contractual relationships with him) and industry wide secrecy (which involves the knowledge of the subject matter among those outside of the owners control).^[43] When the secrecy requirement is mentioned by courts, they typically are referring to internal secrecy.

The secrecy requirement is not absolute. Some disclosures are permissible, but the disclosures are limited to persons who enter into confidential relationships with the owner of the trade secret.^[44] As long as all parties maintain the secrecy, the independent discovery of the information by others need not destroy its protectable status.^[45] If the secret is revealed by dissemination of the product containing it, the trade secret is no longer protected.^[46]

The third requirement of novelty is not as stringent as its counterpart under the patent statutes,^[47] but the novelty in trade secret law is more discriminating than the originality concept under copyright laws.^[48] The degree of novelty will also enter into the determination of damages awarded by the courts.^[49]

The fourth requirement dealing with economic value focuses on such factors as the value of the information, the amount of effort expended in obtaining the trade secret, and the difficulty of acquiring or re-acquiring the trade secret.^[50] In a few instances, heavy reliance on this fourth requirement has resulted in a lowering of the requisite secrecy and novelty standards.^[51]

Federal Preemption of State Trade Secret Law

Although both the definitions and actual requirements of trade secret vary between states, there is a well developed body of trade secret law existing at the state level. This state trade secret law existed for many years, but was recently threatened by a series of Supreme Court cases beginning in the mid-1960's. A brief digression to examine this line of cases is appropriate to better appreciate the position which trade secret law occupies in American jurisprudence.

Sears Roebuck and Co. v. Stiffel Co.^[52] and a companion case^[53] were the first Supreme Court cases in this series which threatened the very existence of state trade secret law. In Sears, a pole-lamp sold by Stiffel Co., had previously been held unpatentable. Sears copied Stiffels' design and sold lamps identical to the Stiffel pole-lamp. Stiffel then sued Sears under the Illinois unfair competition law. The Court stated that an "unpatentable article, like an article upon which a patent has expired, is in the public domain and may be made and sold by whoever chooses to do so."^[54] In broad language threatening the very existence of state trade secret law due to existing federal patent and copyright policy, the Court held that "a state may not, when the article is unpatented and uncopyrighted, prohibit the copying of the article itself or award damages for such copying."^[55]

Five years later in Lear, Inc. v. Adkins,^[56] the Court held that a licensee could not be required to pay royalties under a contract which challenged the validity of a patent. The Court reasoned that requiring such payments would undermine the federal policy favoring full and free use of ideas in the public domain.^[57] In commenting on the theoretical basis of a state enforcing patent licensing contracts, the Court stated that "(a)t the core of this ... is the difficult question whether federal patent policy bars a state from enforcing a contract regulating access to an unpatented secret idea."^[58]

Therefore, although Lear actually rested on a contractual issue of licensees paying under a contract while testing the validity of a patent, the Court again questioned the validity of state trade secret law based on federal pre-emption of this law by the federal patent policy.

In Goldstein v. California,^[59] the Court held that the federal constitutional provision authorizing Congress to grant copyrights for "limited times" was only a limit on Congress and not on the states. Thus a California statute making it a criminal offense to pirate recordings produced by others was not void for lack of a durational limit, despite the federal durational limitation on the Congressional power to grant copyrights.^[60] The key to Goldstein is the Court's conclusion that by congressional silence, Congress indicated that states could regulate copyright matters of a purely local nature. Where the "need for free and unrestricted distribution of a writing is thought to be required by the national interest, the Copyright Clause ... would allow Congress to eschew all protection."^[61] If Congress were to determine that a matter warranted national copyright attention and then preempt the field by concluding that no copyright protection was needed, any state action would be ultra vires which attempted to protect what Congress had intended to be free from restraint.

As seen from Sears, Adkins, and Goldstein the status of state trade secret law was very unclear. During this same time period, the Court decided Gottschalk v. Benson^[62] which has been previously discussed in the patent protection section of this document. Gottschalk invalidated a patent for a computer program converting binary coded decimal (BCD) numerals through the use of a mathematical algorithm. Reading the opinion broadly, one could conclude that all computer programs are unpatentable.^[63] If this extreme position were taken (and this position may be the final outcome after several patent infringement suits reach the Supreme Court)

the combination of Gottschalk with Sears, Adkins, and Goldstein, leads one to conclude that because computer programs are unpatentable, they are outside the area of trade secret protection, and thus unprotected by either federal or state law.

The threat of federal preemption over state trade secret law was eliminated in May of 1974 by the Supreme Court in Kewanee Oil Co. v. Bicron Corp.^[64] Kewanee developed a patentable process which could grow a seventeen inch crystal of a type useful in detection of ionizing radiation. Kewanee decided to forgo patent protection, and instead rely on trade secret law for the protection of this process. Several Kewanee employees signed agreements not to disclose trade secrets obtained while employed for Kewanee. These employees left Kewanee and formed Bicron Corp. which competed with Kewanee in producing the seventeen inch crystals. Based on Ohio trade secret law, the district court granted a permanent injunction against Bicron from producing the seventeen inch crystals. The Court of Appeals, however, reversed on the ground that Ohio's trade secret law was preempted by the federal patent laws.

The Supreme Court reinstated the district Court's opinion by holding that the Ohio trade secret law was not preempted by the federal patent laws. The Court distinguished three types of trade secrets: one known only to its owner not to be patentable, one whose patentability is considered dubious, and one believed by its owner to be a patentable invention. In dealing with the first category of unpatentable inventions, the Court reasoned that there was no public interest in flooding the overburdened Patent Office with applications which would be disapproved. In addition, no public disclosure would occur because patent applications which are denied are kept confidential. Therefore, as to unpatentable inventions, no conflict existed between federal disclosure policy and state protection of this type of trade secret.

Concerning those trade secrets of dubious patentability, the Court invoked the Adkins doctrine that invalid patents are a serious threat "to the free use of ideas already in the public domain"[65] Reasoning from Adkins, the Court concluded that since a licensee of a patent could challenge the validity of a patent, it was better that an invalid patent had never been issued in the first place. The elimination of state trade secret law would bring about the issuance of more invalid patents as in the case of Lear, and thus would have an even greater "deleterious effects on society and patent policy"[66] Consequently, the Court concluded that no spectre of federal pre-emption existed in this second category of dubious patentable trade secrets.

In dealing with the third category of clearly patentable trade secrets, the Court reasoned that the protection available to the owner of an invention through the law of trade secrets is far weaker than that offered by a patent, and consequently the risk that an inventor with a clearly patentable item would opt for trade secret protection and avoid disclosure is remote indeed.[67]

Thus the Court validated all three types of trade secrets despite the federal policy of disclosure.[68] Unless Congress takes affirmative action, state trade secret law is not preempted by federal patent policy.

Software and Trade Secrets

With the very existence of state trade secret law settled in light of Kewanee, it is appropriate to return to the four requirements of trade secrets [1) appropriateness of subject matter, 2) secrecy, 3) novelty, and 4) economic value], to determine their applicability to the special case of software. Computer programs clearly fall within the first requirement of appropriateness of subject matter. Most authorities allow trade secret protection of those entities within the "processes," "mechanism," and "compounds" class,[69]

and therefore, any completed program is protectable. Those programs which are in the developmental stage are not as safe as completed programs, but "as the idea becomes more detailed and moves toward implementation, it is more likely to be regarded as qualified for trade secret protection."^[70] Mere documentation and data in the form of programs will probably fall in the least protectable class of "information, involving no element of novelty or discovery, but of value to its owner."^[71]

In order to insure fulfillment of the secrecy requirement, special care must be taken by the owner both in the case of maintaining in-house secrecy and in the case of selective proliferation of the program. Unintentional duplication of programs is commonplace, and thus in the case of in-house secrecy, the owner should ensure limited access to the program. Relevant documents should be stamped as secret or confidential. Public statements about developments should be cleared in advance through a legal officer, and careful records should be kept of all persons to whom the information is disclosed.^[72] Secrecy is frequently the key issue in trade secret litigation, therefore, these safeguards must be taken seriously.

Similarly, in the case of a sale or rental of a program package, the owner should contract with the vendee to insure that disclosures are limited and closely controlled to protect the trade secret status of the program package. Various methods are available to facilitate maintaining this secrecy including 1) only allowing the transfer of object code, 2) limiting the amount of documentation transferred with the package, 3) establishing a licensing system on an individual installation basis, and 4) contractual provisions to limit the grantee or licensee in proliferation of the program from the installation site.

Very little has been written on the novelty requirement of computer programs for trade secret protection due to the limited case law dealing specifically with trade secret protection of computer

software. It would appear, however, that if a program involves many complicated subroutines, the novelty requirement would be satisfied.

The fourth requirement of value hinges on the value both in monetary and non-monetary terms which the program has. The greater the value of the program, the wider the scope of protection afforded by the law of trade secrets.^[73] Consequently, it behooves the owner to establish a detailed log for each use of the program to provide tangible evidence of its value. The log will establish that such efforts were worth the time and energy of the owner, and thus implicitly, that the program is valuable. Establishing the actual development costs of the program is also an important element in ensuring common law protection.

Scope of Protection

The Restatement of Torts outlines the protection given by trade secret law. Generally a person is liable for the use or disclosure of another's trade secret when he either discovers the secret by improper means, or breaks a confidence which he has with others. Further, an individual is liable, if with full knowledge of the facts, he learns the secret from a third party. Finally, if disclosure is accidentally made to an individual, and the individual is informed of the facts, the individual is liable if he uses the trade secret.^[74] In the case of innocent discovery of the secret, a person is not liable for his own use of the secret until he receives notice of the mistaken disclosure.

A common method to protect computer software is the use of restrictive contractual agreements between the owner of the trade secret and all others with whom he deals.^[75] The two distinct categories of such contractual agreements are employee and non-employee contracts. Clauses in employee contracts requiring non-disclosure both during employment and after employment are commonly used.^[76]

These clauses are hardest to enforce when trained employees with valuable skills are involved.^[77] Another common device used in employee contracts is the non-competition clause. These clauses simply limit an employee from competing with the employer for a definite time period and within a specified geographic area once the employee terminates his relationship with the employer. Courts have applied a rule of reason to both time and geographic limitations. The reasonableness of the time period in restrictive agreements will vary between jurisdictions, and may vary depending on the type of position held by the employee.^[78] Traditionally, geographic limitations have been viewed as the competitive region of the employer, but the software industry is national in scope, and thus national territorial limitations should be valid.^[79]

Non-employee contracts are more difficult to deal with. A confidential relationship is less likely to be implied with non-employees, and thus specific contractual provisions with leasees and vendees are essential to ensure successful protection. If the owner chooses to lease his program on a non-exclusive basis, the leasee will only acquire the right to use the program while title remains in the lessor. In the contract, the leasee should agree to prevent intentional and unintentional disclosures to third parties. The time period of the lease as well as the method of disposition of the transferred materials at termination of the lease should also be specified.

If the developer chooses to sell the software, full title and exclusive rights will be transferred to the vendee. In this case the vendor must agree to forego use and disclosure of the program once the sale is finalized. Unnecessary litigation can be avoided by specifying the exact terms of the transaction in the contract.

A transaction similar to outright sale of software is a contract for development of a program. Problems arise, however, from the fact that the subject matter of the contract (technically known

as the res) does not exist at the time of execution of the contract. In this relationship, title may reside in either party to the contract, and therefore, the division of rights should be clarified before execution of the contract. Matters such as the rights which the developer has in using variations of the program for other contracts should be clarified.^[80]

Although outside the scope of this document, once a contract to license, sell, or develop is under consideration, there are many additional legal implications. The normal legal provisions of contract law enter into each contract such as warranty liability and penalties for late completion. Careful thought must be given to tax implications of the contract as well as other legal areas such as antitrust considerations. All of these matters will not be further developed at this point due to the vast amount of literature in the field and the impossibility of considering all aspects for each contract.

Criminal and Non-Criminal Remedies Under Trade Secret Law

On the civil side, the owner of a trade secret may obtain injunctive relief to prevent an appropriator from either disclosing the secret to a third party or using the secret himself.^[81] If the secret has already been disclosed to a third party or used by the appropriator, the owner may seek damages resulting from the disclosure or from the profits accrued by the use of the trade secret.^[82] In a recent case on trade secret protection of computer equipment including software, the court in Telex v. IBM^[83] held that Telex had violated the Oklahoma trade secret law and thus ruled in favor of IBM's counter claim against Telex.^[84]

A relatively new aspect of trade secret protection is the use of state criminal sanctions. A financially destitute employee with little to lose economically, may consider appropriating a trade secret if the risk is only a civil injunction or a civil action for

damages.^[85] The damage done to a developer can be considerable, and thus many states have added criminal penalties as an additional deterrent against trade secret theft. Two methods of providing such sanctions presently exist: criminal prosecution for software theft if the stolen information is in such a form as to fit the relevant language of the existing statute, and specific criminal sanctions for misappropriation of trade secrets.^[86] The first category of general statutory sanctions may be further divided into those jurisdictions which define the subject matter of theft in terms of property,^[87] those jurisdictions which qualify or extend (in the form of lists) the property concept in the relevant statutes,^[88] and those jurisdictions which provide statutory protection for things of value.^[89]

Three complications arise when these statutes are used to protect trade secrets. First, many of the statutes do not carry significant penalties (if at all) for theft involving an "intent to return," and thus the appropriator might easily take the program, copy it, and then return it. Thus the damage would have been done, but the appropriator would be immune from criminal prosecution under the general statutes.^[90] Second, if the relevant statutory wording only includes the article in which the secret is embodied (i.e., magnetic tapes or sheets of paper), the protection is worthless. Third, the trade secret must qualify for protection or the statute will be impotent against appropriation by memory rather than copying of the information.

At the federal level, no express trade secret statutes exist. There are, however, statutes which prohibit the transportation^[91] and sale or receipt^[92] of stolen goods, wares, merchandise, securities, or money. The problems raised under the discussion of state larceny statutes are also pertinent under the federal statutes. It is still not settled whether the theft of computer programs falls under the federal statutes.^[93] Further, no protection exists under these statutes against appropriation by memory.^[94]

Overall, trade secret protection of software is a viable alternative for private industry.^[95] Although trade secret protection has serious limitations, it currently appears to be the best alternative for private enterprise.^[96]

THE UNIVERSITY ENVIRONMENT AND PROTECTION OF SOFTWARE

As universities become more heavily involved in software development, they must determine if they want to legally protect the software they develop. If the university policy is to legally protect the software which has been developed for commercial use, then there are three alternatives. As previously discussed, the area of patent protection is currently very unsettled. Even those patents which are being granted may later be invalidated in an infringement suit. Copyrights also present problems in that the amount of real protection afforded by a copyright is still unknown. At first blush, therefore, trade secret law appears the most viable method to protect software which a university has developed and to which the university has title.

A full discussion of all policy considerations of trade secret protection of software in a university environment is beyond the scope of this document, however, a few of the advantages and disadvantages in the use of trade secret protection merit brief attention. Assuming the profits from the project are shared with the university personnel who developed the software, the remaining funds accrue to the state university at no expense to the taxpayer. On the negative side, one can argue that the goal of the university should not be a business of exploiting business ventures, but rather should be one of education. Therefore, the university policy should be one of public dedication of all software which is developed at the university rather than trade secret protection of the software and commercial sale of the software.

Assuming for the moment that the university policy is to use trade secret laws to protect software which is developed for commercial sale, this policy is fraught with danger. First, employment agreements would have to be established in which faculty members agreed to maintain the confidentiality of any software which they developed. Next, all publications would have to be censored which dealt with the software being protected by trade secret. Finally, all research done on protected software would have to be done under lock and key. It should be noted, however, that the censorship and lock and key research requirements are not new to the university in that some government sponsored research and development is done in the university environment which requires these types of security measures.

The establishment of proper incentives for software development in a university environment is also a difficult problem. Three general types of incentives exist. First, at the beginning stages of an individual's career, acceptance in his field will be sufficient incentive. It should be noted, however, that the power of this incentive quickly diminishes as the individual becomes accepted in his field. Second, as an individual successfully develops software, he can be advanced within the organization, and thus the individual will receive both monetary gains as well as peer group approval as incentive for further software development. Again, however, the power of this second type of incentive diminishes as an individual reaches higher levels of the organization. Finally, there can be some type of direct payment to university personnel for the development of software.

At present the University of Illinois does not have a formal procedure to reward university personnel who successfully develop software. The General Rules Concerning University Organization and Procedure,^[97] only provide a modest incentive for development of patentable ideas and authorship of copyrightable material. The Procedure on Patent Matters of The General Rules is the key provision in payment to inventors and reads as follows:

The determination as to what portion of net income shall be paid to the inventor or discoverer, after the payment of costs of securing a patent and of development and administration, from a patent held by the University or transferred by it to the University of Illinois Foundation shall be studied by the University Patent Committee; which shall make a recommendation to the President. In most cases, the University contribution in use of facilities and resources will be significant and, therefore, the inventor will have little real claim to compensation over his regular University salary. In some cases, the University Patent Committee shall recommend that the proportion of net income assigned to the inventor shall fall in the range of 10 to 15 per cent of net income. In unusual cases, in which the University contribution is obviously less, this percentage allocation to the inventor may go to 25 per cent and, in rare cases, the rate may be higher. (emphasis added)[98]

The use of net income is critical, in that the inventor has little control over the expenses which the University incurs in the administration and development of his patent.

The Copyright and Recordings section of The General Rules provides the framework for payment to authors who copyright material. The main section reads as follows:

A University Committee on Copyrights and Recordings, appointed by the President, will review the circumstances involved in each case that might arise under the principle stated in (e), [the use or sale of copyrighted material resulting in net income to the University] and make recommendation concerning it to the President and Board of Trustees. It is expected that the Committee will be guided in its recommendations by standards analogous to those stated in Section 18(c) concerning patents.[99]

Therefore, at present the University of Illinois does not have a formal procedure to reward and encourage software development, but provisions do exist to encourage, on modest levels, the development of patentable inventions and copyrightable material.

Academic Freedom

The secrecy measures necessary for the trade secret protection of software conflict with the general principles of academic freedom, rights and freedoms of students, and professional ethics of faculty. For example, the University of Illinois Statutes state that:

It is the policy of the University to maintain and encourage full freedom, within the law, of inquiry, discourse, teaching, research and publication and to protect any member of the academic staff against influences, from within or without the University, which would restrict him in the exercise of the freedoms in his area of scholarly interest. [100]

The 1940 Statement of Principles on Academic Freedom and Tenure of the American Association of University Professors and the Association of American Colleges states:

Institutions of higher education are conducted for the common good and not to further the interest of either the individual teacher or the institution as a whole. The common good depends upon the free search for truth and its free expression.

Academic freedom is essential to these purposes and applied to both teaching and research ... Academic freedom in its teaching aspect is fundamental for the protection of the rights of the teacher in teaching and of the student to freedom in learning.

(a) The teacher is entitled to full freedom in research and in the publication of the results subject to the adequate performance of his other academic duties, but research for pecuniary return should be based upon an understanding with the authorities of the institution. (emphasis added and footnotes omitted)[101]

The preamble of the Joint Statement on Rights and Freedoms of Students of the American Association of University Professors, the National Association of Student Personnel Administrators, the United States National Student Association, the American Association of Colleges,

the Association of American Colleges, and the National Association of Women Deans and Counselors states:

Freedom to teach and freedom to learn are inseparable facets of academic freedom. The freedom to learn depends on appropriate opportunities and conditions in the classroom, on the campus, and in the larger community.[102]

Finally, the Statement on Professor Ethics of the American Association of University Professors emphasizes the need for complete academic freedom by stating:

As a member of his institution, the professor seeks above all to be an effective teacher and scholar. Although he observes the stated regulations of the institution, provided they do not contravene academic freedom, he maintains his right to criticize and seek revision. [103]

As one can see, the use of trade secret law to protect software in a university environment has major obstacles. Overall, the only solution is to examine each case on an individual basis. A balance must be made between the right of students to learn in an environment unburdened by security measures, the right of faculty to teach and do research, and finally the right of society to receive the maximum return on all resources spent on universities. The balance is an extremely difficult one to draw, and only time will tell the eventual outcome of such considerations.[104]

GOVERNMENT PROCUREMENT OF SOFTWARE

An additional area of concern is the relationship between both private and public suppliers of software and the federal Government. One of the main reasons the Federal Government must contract for development of software is the high manpower costs of properly trained computer personnel. Salaries of twenty to twenty-five thousand are common for qualified personnel, but the present civil service salary system cannot easily accommodate such high salaries.[105]

Although direct sales of pre-developed software protected under patents or copyrights would be the best legal method to contract with the Government for software, such situations are atypical.^[106] The normal situation is for the Government to contract for the development of software. There are three main methods to contract for software development.^[107] First, a software firm may contract to supply trained personnel on a daily basis to develop software for the Government. If this is done, it is reasonably clear that the Government is entitled to exclusive rights to all software developed by the software personnel. Another method is to bid for a contract, but to include a cost plus clause in which the Government agrees to absorb any additional costs above a certain figure under various conditions of cost overruns. Again, the Government pays for everything and thus it is reasonably clear that the Government would acquire exclusive rights to the contract.

The third approach is to contract for software development, but the cost is a fixed item in the contract. If the Government supplied all of the resources to develop the software, then the Government should be entitled to exclusive rights in the software. The difficulty arises when the software developer supplies some of the resources in the software development.

Patent Rights and Rights to Data Clauses

In most government contracts for research and development and governmental supply, two types of provisions outlining the government's rights to intellectual property are included.^[108] These two provisions are the patent and data clauses. The patent provision, usually entitled the Patent Rights clause, requires that the contractor supply the Government written disclosure of each invention conceived of under the contract or the first reduction to actual practice. Most rights which the Government has under the patent clause are specifically spelled out, but these specified rights do not presently cover

software. NASA had adopted a broader patent provision referred to as the New Technology clause^[109] which replaces the traditional Patent Rights clause. The New Technology clause requires the reporting of all inventions, and in addition, the reporting of all innovations.

The data provision, usually entitled the Rights in Data clause, is used in most Government contracts where the delivery of data is specified. This clause does not specifically call for acquisition of any data, but rather defines the rights which the government has in the specified data. The rights which the government has under the Rights in Data clause are either limited to very specified uses, or unlimited.^[110]

Delivery of computer programs may be specifically required in the contract, or delivery provisions may be included under the general patent provision. Thus the rights which the Government has in any computer programs developed under the contract depend on whether the patent or data provision of the contract is used.

As can be seen from this general discussion, no specific contract provisions currently exist which explicitly define the rights of each party to a Government software procurement contract. An example of this ambiguity can be found in McDonnell Automation Co.^[111] in which the Air Force contracted for a computer program to aid Air Force attorneys in researching various federal statutes. After the system, entitled Legal Information Through Electronics (LITE), was developed, the contractor protested when the Government exerted unlimited rights to the program under the Rights in Data clause. The Comptroller General held that the Government was entitled to an unlimited license to the program under the Rights in Data clause. With proper contract provisions dealing with computer programs, this case and many unreported disputes could be avoided in Government procurement law.

Software Revision to ASPR's

In response to the need for a specific contract provision dealing with computer programs the Armed Services Procurement Regulation Committee issued a proposed change to the Armed Services Procurement Regulation (ASPR) in September of 1973.^[112] Much debate has occurred over this proposal, and final issuance of a new ASPR on computer programs has not occurred.

Assuming a contractor negotiates a limited Rights in Data clause with the Government, the contractor must still determine the type of legal protection which he will use to protect his software. Currently, the most viable method to use in protection of computer programs is trade secret law. Until recently, it was an axiom of Government contract law that the exclusive remedy for governmental breach of a contract providing for limited use of proprietary data^[113] was a damage action in the Court of Claims pursuant to the Tucker Act.^[114] This belief was recently shattered in International Engineering Co. v. Richardson^[115] in which plaintiff sought to enjoin the Government's misuse of proprietary information. The district court held that it did have jurisdiction and did grant an injunction against the Government's misuse of the proprietary information.

Other remedies for the Government's misuse of proprietary information include requests to the General Accounting Office to have the Comptroller General order cancellation of bids (or requests for bid proposals) if proprietary data is being disclosed by the Government.^[116] The Boards of Contract Appeals is another alternative to prevent the Government's misuse of proprietary data.^[117] The Boards, however, only have jurisdiction over current contracts. Finally, a suit for unauthorized use of proprietary information could be brought in the Court of Claims.^[118] Damages would then have to be assessed, based on the damage sustained by the victim or by the profits earned by the wrongdoer who used the misappropriated material. The latter

course of action, however, is unappealing due to the fact that the secrecy of the computer program is lost, and thus future use of the program under trade secret protection is impossible.

Once the ASPR software regulation is issued, future contracts with the Government should become better defined. In addition, if the present case law develops and allows injunctive relief in federal District court, the protection of software through trade secret law will be more viable due to the immediate availability of judicial remedy through injunctive relief.

CONCLUSION

Although many alternatives exist for the legal protection of software, no definite answer exists for the best method to protect software in both the public and private sectors of the economy. On the private side of the economy, a developer of software may be able to obtain patent protection if the computer program is related to a mechanical device and falls under the line of cases currently being decided by the Court of Custom and Patent Appeals. It should be noted, however, that the true test of these patents will be in an infringement suit. Next, copyright protection may be an alternative, and as seen in the recent Telex v. IBM, such protection has withstood the first test at the district court level. At present, probably the optimal technique to protect software due to the uncertainties of patent and copyright protection is through the use of trade secret law. The use of trade secret law, however, is by no means without difficulty. In contracts between private developers and the Government, trade secret protection is more viable today due to the recent case law allowing injunctive relief against the Government for misuse of trade secret data by the government. The revision of the ASPR regulations on computer programs will also help clarify this situation.

On the public side of a university developing computer software for commercial sale, the picture is even less clear. The university must face the legal obstacles of either patent, copyright, or trade secret protection which the private sector has to consider. In addition, if the university were to adopt trade secret protection of software, the university must resolve the conflict between trade secrets and academic freedom. Even if all of these issues could be resolved, there is no definitive answer as to the contractual relation between a university and the Government in contracting for software in which the university has contributed some of its own resources in the development of the software.

The computer industry is dynamic, and the most rapid growth now occurring in the industry is in software development. Software technology has outgrown the legal development of software protection. Thus in the foreseeable future, the legal protection and regulation of software will remain in a state of flux until major solutions evolve which permit an intelligent and rational method to protect computer software.

NOTES

- [1] Bauer, "Software Markets in the 70's," Expanding Use of Computers in the 70's: Markets--Needs--Technology, (ed by Grunberger, 1971).
- [2] Auerbach, "Technological Forecast," Expanding Use of Computers in the 70's: Markets--Needs--Technology, (ed by Grunberger, 1971).
- [3] See generally, Bower, "Market Changes in the Computer Services and Industry," 4 The Bell Journal of Economics and Management Science 539 (1973).
- [4] See e.g. George Washington University, Computers in Law Institute, The Law of Software (1968 and 1969). For an up to date bibliography on software protection see American Bar Association, Section of Patent, Trademark and Copyright Law, 1974 Committee Report (prepared for the 1974 ABA Meetings August 12-15, 1974) [hereinafter ABA, 1974 Report].
- [5] Hardware clearly falls under the statutory definition of a machine or manufacture. 35 U.S.C. § 101 (1970).
- [6] See e.g. S. 1360, 93rd Cong., 2nd Sess. See also ABA, 1974 Report for a discussion of various parts of these proposals to amend the existing patent laws.
- [7] Mackay Co. v. Radio Corp., 306 U.S. 86, (1938).
- [8] See e.g. Cochrane v. Diener, 94 U.S. 780 (1876); O'Reilly v. Morse, 15 How (56 U.S.) 62 (1853).
- [9] Woodcock, "Mental Steps and Computer Programs," 52 J. Pat. Off. Soc'y. 275 (1970).
- [10] See Note, 14 Boston Coll. Ind. and Comm. L. R. 1050 (1973); Note, 4 Loyola Univ. of Chicago, L. J. 560 (1973).
- [11] Commission on Patent System, The 1966 Report of the President's Commission on the Patent System (reprinted in S. Doc. No. 5, 90th Cong., 1st Sess. p 21).
- [12] 409 U.S. 63 (1972).

- [13] Congress defined the categories of discoverers and inventions for which patents may presently be granted:

The term "process" means process, art or method, and includes a new use of a known process, machine, manufacture, composition of matter, or material. 35 U.S.C. § 100(b).

In addition, 35 U.S.C. § 101 provides:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefore, subject to the conditions and requirements of this title.

- [14] Application of Benson, 441 F.2d 682 (C.C.P.A. 1971).
- [15] See Note, 4 Loyola Univ. of Chicago L. R. 560, 575 (1973).
- [16] See Application of Brandstadter, 484 F.2d 1395 (C.C.P.A. 1973); Application of Doyle, 482 F.2d 1385 (C.C.P.A. 1973); Application of Comstock, 481 F.2d 905 (C.C.P.A. 1973); Application of Knowlton, 481 F.2d 1357 (C.C.P.A. 1973).
- [17] See Application of Musgrave, 431 F.2d 882 (C.C.P.A. 1970); Application of Mahony, 421 F.2d 742 (C.C.P.A. 1970); Application of Bernhart, 417 F.2d 1395 (C.C.P.A. 1969); Application of Prater, 415 F.2d 1393 (C.C.P.A. 1969).
- [18] The Canadian Government recently issued a patent on a computer program. See Computerworld p 1 (August 7, 1974). If any foreign government upholds a patent on a computer program, the patent may be valid in the U.S. under the various patent treaties. See generally ABA, 1974 Report 287.
- [19] Galbi, "Software and Patents: A Status Report," Computer Law Service § 4 - 2, art. 1 (ed by Bigelow, 1974).
- [20] For a concise legislative history of copyright law see footnote 17 in Goldstein v. California, 412 U.S. 546, 562 (1973).

- [21] See Generally, Nimmer, Nimmer on Copyrights (1974) [hereinafter Nimmer], Nicholson, A Manual of Copyright Practice for Writers, Publishers, and Agents (2nd ed. 1970).
- [22] Nimmer, § 111.
- [23] Under the recently passed Senate revision bill of the copyright law (S. 1361, 93rd. Cong., 2nd Sess.), the duration of copyright protection would be 50 years after the author's death for both common law and statutory copyright rather than the existing perpetuity period for common law copyrights and 56 years for statutory copyright.
- [24] Nimmer, § 112.
- [25] Under the Senate revision bill (S. 1361, 93rd. Cong., 2nd Sess.), the statutory duration would be changed to the life of the author plus 50 years.
- [26] Nimmer, §§ 150 and 151.
- [27] See Bigelow, Computer Law Service (1974) appendix 4-3a for a reprint of the circular.
- [28] See generally, Note, "Copyright Protection for Computer Programs," 64 Colum. L. R. 1274 (1964). The Senate recently passed a bill (S. 1361, 93rd. Cong., 2nd Sess.) revising the existing copyright statutes. Computer programs are proper subject matter under the proposed bill. Section 117 is the key provision and states:

Notwithstanding the provisions of sections 106 through 116, this title does not afford the owner of copyright in a work any greater or lesser rights with respect to the use of the work in conjunction with automatic systems capable of storing, processing, retrieving, or transferring information, or in conjunction with any similar device, machine, or process, than those afforded to the works under the law, whether title 17 or the common law or statutes of a state in effect on December 31, 1974, as held applicable and construed by a court in an action brought under this title.

- [29] Galbi, "Copyright and Unfair Competition Law as Applied to the Protection of Computer Programming," Computer Law Service, § 4-3, art. 1, p 17 (ed by Bigelow, 1974).
- [30] 367 F. Supp. 258 (N.D. Okl. 1973).
- [31] 310 F. Supp. 1073 (W.D. Wash. 1969)
- [32] See Galbi, "Copyright and Unfair Competition as Applied to the Protection of Computer Programming," Computer Law Service, § 4-3, art 1, p 18 (ed by Bigelow, 1974).
- [33] Galbi, "Proposal For New Legislation to Protect Computer Programming," 17 Bull. Copyright Soc'y. 280 (1970); Morris, "Protecting Proprietary Rights of Computer Programs: The Need For New Legislative Protection," 21 Catholic Univ. L. R. 181 (1970) [hereinafter Morris].
- [34] Williams & Wilkens v. U. S., Docket No. 73, 1279 (487 F.2d 1345) (U.S. Ct. Clms.) is presently before the Supreme Court. In Williams the National Institute of Health made over one million single copies of various obscure medical journal articles, some of which Williams & Wilkens had copyrighted. With a strong dissent, the U.S. Court of Claims held 4-3 that the photo copying of a copyrighted article, one copy at a time, was not an infringement of the copyright. Therefore, the outcome of this case will undoubtedly affect the status of software copyright protection.
- [35] Bender, "Trade Secret Protection of Computer Software," 38 Geo. Wash. L. Rev. 909, 926 (1970) [hereinafter Bender].
- [36] Restatement of Torts, § 757, comment (b), (1939). See also Mycalex Corp. v. Pemco Corp., 64 F. Supp. 420, 423 (Md. 1946).
- [37] Victor Chemical Works v. Iliff, 299 Ill. 532, 545 (1921). The identical quote was used again in Schulenburg v. Signatrol, Inc., 33 Ill. 2d 379, 385 (1965), cert.denied. 383 U.S. 959 (1966).
- [38] 198 U.S. 236, 250 (1905). See also Ellis, Trade Secrets § 12, (1953) [hereinafter cited as Ellis] which states:

The common law gives a man the right to keep his ideas or the results of the work he has done, or paid for doing, to himself. The fact that others are at liberty to do similar work, if they wish, does not authorize them to steal his. The principle is fundamental. The broad terms 'ideas' and 'work' are used in stating it, instead of the more usual one 'trade secrets,' since the latter is frequently interpreted as something akin to an unpatented invention.

- [39] Dupont Power Co. v. Masland, 244 U.S. 100, 102 (1917).
- [40] See generally, Wessel, "Legal Protection of Computer Programs," 43 Har. Bus. Rev. 97 (March-April, 1965) (hereinafter Wessel). Several of these requirements are discussed in Kewanee Oil Co. v. Bicron Corp., _____ U.S. _____, 94 S. Ct. 1879 (1974).
- [41] Turner, The Law of Trade Secrets 12 (1962) [hereinafter cited as Turner].
- [42] See B. F. Goodrich Co. v. Wohlgemuth, 117 Ohio App. 493 (Ct. App. 1963); Kaumagraph Co. v. Stampagraph Co., 235 N.Y. 1 (1923); National Tube Co. v. Eastern Tube Co., 3 Ohio Ct. C. Rep. N.S. 459 (Cir. Ct. 1902), aff'd, 69 Ohio St. 560, 70 N.E. 1127 (1903).
- [43] Bender, 928.
- [44] Morris, 195. See also DuPont Powder Co. v. Masland, 244 U.S. 100, (1917); General Aniline and Film Corp. v. Frantz, 50 Misc. 2d 994, 274 N.Y.S. 2d 634, 151 U.S.P.Q. 136 (N.Y. Sup. Ct. 1966); Cincinnati Bell Foundry Co. v. Dodds, 10 Ohio Dec. Rep. 154 (Super. Ct. 1887).
- [45] Bender, 928.
- [46] See Wesley-Jessen Inc. v. Reynolds, _____ F. Supp. _____ (Ill. 1974), 182 B.N.A. Pat., Trademark, and Copyright J., A-2 (June 13, 1974) (trade secret no longer a trade secret if embodied in a product which is then sold and examined with reverse engineering techniques). See also Oppenheim, Cases on Unfair Trade Practices 237 (2d ed. 1965).

- [47] W. R. Grace & Co. v. Hargadine, 392 F.2d 9 (6th Cir. 1968) (comparison of patent and trade secret novelty requirement). Bender, at note 101, gives an example of the nature of patent novelty:
- Consider an invention which no one alive has anticipated; and the patent for which reads no prior art. If, one year after the patent issues, an archeologist discovers an old Indian cave in Arizona with wall paintings disclosing that invention, the patent is invalid for lack of novelty. Such is the absolute nature of patent novelty. Bender, 929.
- [48] Alfred Bell and Co. v. Catalda Fine Arts Inc., 191 F. 2d 99 (2d Cir. 1951) (example of copyright novelty). Bender again states: "For a copyright it will suffice that the author contributed more than a merely trivial variation, i.e., something of 'his own'." Bender, note 100, at 939.
- [49] Bender, 929.
- [50] See Wessel, 100.
- [51] Ellis, § 14.
- [52] 376 U.S. 225 (1964).
- [53] Compco Corp. v. Day-Brite Lighting, Inc., 376 U.S. 234 (1964).
- [54] 376 U.S. at 231
- [55] 376 U.S. at 232.
- [56] 395 U.S. 653 (1969).
- [57] The Court noted the heavy economic burden involved in patent litigation, and therefore, the extra burden of the royalty payments could deter most attempts to challenge patents. In particular, the Court stated:
- The deterrent effect would be particularly severe in the many scientific fields in which invention is proceeding at a rapid rate. In these areas, a patent may well become obsolete long before its 17-year term has expired. If a licensee

has reason to believe that he will replace a patented idea with a new one in the near future, he will have little incentive to initiate lengthy court proceedings, unless he is freed from liability at least from the time he refuses to pay the contractual royalties. 395 U.S. at 673-4.

[58] 395 U.S. at 672.

[59] 412 U.S. 546 (1973). Chief Justice Burger, writing for the majority, merely distinguished Sears and Compco from Goldstein. Dissents by Justice Douglas and Justice Marshall (each concurred in by Justice Brennan and Justice Blackmun), however, rely on Sears and Compco.

[60] 412 U.S. at 560-561.

[61] 412 U.S. at 559.

[62] 409 U.S. 63 (1972).

[63] Kaul, "And Now State Protection of Intellectual Property?" 60 A.B.A.J. 198, 200 (February 1974) stated:

While some observers have expressed the view that Benson did not completely bar protection of computer programs, it is extremely doubtful whether valid protection is possible under the patent laws as they are now written.

[64] _____ U.S. _____, 94 S.Ct. 1879 (1974).

[65] _____ U.S. at _____, 94 S.Ct. at 1889.

[66] _____ U.S. at _____, 94 S.Ct. at 1890.

[67] One should note, however, that trade secrets such as the Coca Cola secret formula are patentable, but through the use of trade secret protection, these ideas can be protected for periods longer than the 17-year patent protection period.

[68] For a discussion of the future of trade secrets after Kewanee see 182 B.N.A. Pat., Trademark, and Copyright J., A-9 (June 13, 1974)

- [69] 43 C.J.S., Injunctions, § 148 (1945).
- [70] See Irizarry y Puente v. Harvard College, 248 F.2d 799, (1st Cir.), cert. denied, 356 U.S. 947 (1957); Hamilton National Bank v. Belt, 210 F.2d 706, (D.C. Cir. 1953).
- [71] Bender, 927.
- [72] Wessel, 100.
- [73] Ellis, § 14.
- [74] See Restatement of Torts, § 757 (1939).
- [75] See Doerfer, "The Limits on Trade Secret Law Imposed by Federal Patent and Antitrust Supremacy," 80 Harv. L. Rev. 1432 (1967) [hereinafter Doerfer].
- [76] Bender, 934.
- [77] See Note, "Developments in the Law - Competitive Torts," 77 Harv. L. Rev. 888 (1964). Doerfer at note 16 states:
- Trade secret controversies growing out of employment relationships present special difficulties. The interest in allowing an employee to move from job to mob without allowing his employers to claim a proprietary interest in the skills acquired during his stay must be balanced against the interest in permitting the holder of a competitive advantage to make a limited disclosure of his secret in order to exploit it. A former employee may continue to use general knowledge, but not secrets, acquired in his work; no explicit agreement is necessary to enable a former employer to restrain disclosure.
- [78] See Klein, "The Technical Trade Secret Quadrangle: A Survey," 55 Nw.U.L.Rev. 437 (1960).
- [79] 10 Cavitch, Business Organizations § 234.02 (1974).
- [80] Id., § 233.02.

- [81] See Kewanee Oil Company v. Bicron Corporation, _____ U.S. _____, 94 S.Ct. 1879 (1974); Schulenburg v. Signatrol, Inc., 33 Ill. 2d 379 (1965), cert. denied 383 U.S. 959 (1966)(although an injunction is a drastic remedy, it may be granted in appropriate instances). See also, "Software, Statutes, and Stare Decisis," 13 How.L.J. 420 (1967).
- [82] See Morris 195.
- [83] 367 F. Supp. 258 (Okla. D.C. 1973).
- [84] Id., Conclusion # 48.
- [85] Bender states:
- When the secret can be utilized by the thief with only a nominal investment, the possibility of civil suit may prove to be an empty threat. A software house is perhaps the best example of a business requiring a low initial investment of capital. To launch his own software house, one needs only a programmer, a pad, and a pencil. Thus, especially if he happens to be a programmer, an employee who turns thief may have precious little of an investment to lose as a result of a lawsuit. Bender, 942.
- [86] The Illinois definition of property also includes trade secrets, Ill. Rev. Stat., ch. 38, § 15-1 (1974).
- [87] These include Oregon, Utah, Idaho, and Kentucky. In addition, Bender states:
- In any of these four jurisdictions only strict attention to the wording and comprehension of interpretive cases will indicate whether the larceny statute can be used to prosecute theft of a trade secret. Bender, 945.
- [88] These include Alabama, Alaska, Arizona, Connecticut, Delaware, Indiana, Iowa, Mississippi, Nevada, North Dakota, Rhode Island, South Carolina, South Dakota, Texas, Vermont, Washington, West Virginia and Wyoming. Bender, 945.

- [89] These include District of Columbia ("anything of value"), Florida ("article of value of any kind"), Hawaii ("anything of marketable, saleable, assignable, or available value") Kansas ("valuable thing whatsoever"), Louisiana ("anything of value"), Maryland ("thing"), Missouri ("valuable thing"), Montana ("article of value of any kind"), and Virginia ("money or other thing"). In addition, Bender states that:
- Prosecution will generally be easier under these statutes than under those using the word 'property,' since it should be easier to show that a trade secret is a thing of value than to show it is property. Bender, 946.
- [90] For a recent case in which the defendant was convicted under a felony theft statute rather than a specific trade secret theft statute, see *Hancock v. Texas*, 402 S.W. 2d 906 (Texas Crim. App. 1966), 379 F.2d 552 (5th Cir. 1967) (defendant's petition for habeas corpus denied at district court and his appeal to the 5th Cir. also denied).
- [91] 18 U.S.C. § 2314 (1970).
- [92] Id., § 2315.
- [93] In several cases the courts have held that the act of transporting photostatic copies of the stolen information (not computer programs) violated the federal statutes. See e.g., *United States v. Greenwald*, 479 F.2d 320 (6th Cir.), cert denied, 414 U.S. 854 (1973); *United States v. Bottone*, 365 F.2d 389 (2d Cir. 1966), cert. denied, 385 U.S. 974 (1966); *United States v. Lester*, 282 F.2d 750 (3rd Cir. 1960), cert. denied, 364 U.S. 937 (1961).
- [94] See *United States v. Bottone*, 365 F.2d 389, (2d Cir. 1966) (court commented that 15 U.S.C. 2314 would not apply to the theft of trade secrets by memory).
- [95] It is generally conceded that patent protection is better than trade secret protection for computer programs. See Sheers and Encke, "Copyrights of Patents for Computer Programs?", 49 J. Pat. Off. Soc'y 323 (1967).
- [96] For more discussion of the advantages and disadvantages of trade secret protection of computer programs see Morris 197.

- [97] The General Rules Concerning University Organization and Procedure (revised May, 1972). [hereinafter The General Rules].
- [98] Id. § 18(c).
- [99] Id. § 19(f).
- [100] University of Illinois Statutes, Art. X, § 2(1972).
- [101] 56 A.A.U.P. Bulletin 323,324 (Autumn 1970).
- [102] 54 A.A.U.P. Bulletin 258 (Summer 1968).
- [103] 55 A.A.U.P. Bulletin 86 (Spring 1969).
- [104] For an earlier treatment of difficulties encountered by universities in managing research see Palmer, University Research Problems (1949 and 1962). The developers of PLATO IV have proposed a compensation arrangement for developers of course related software (courseware) which uses copyright protection. Under this proposed plan, the University of Illinois would receive 20 percent of gross revenue while the author would receive the remaining 75 percent of gross revenue. The accent is on gross revenue, in that the author will have more control over his courseware than under the University Copyrights and Recordings provision where University administrative expenses would reduce the gross revenue to zero net revenue. If the author was commissioned by the University to develop the courseware under a released time arrangement, the University's share would be increased to 60 percent of gross revenue, while the author's share would be reduced to 40 percent of gross revenues. Finally, if some one unrelated to the University developed courseware, the University would receive 80 percent of gross revenue while the author would receive the remaining 20 percent. This procedure avoids the trade secret problems previously discussed and also provides reasonable incentive for courseware development. The problems encountered in the regulation of courseware, however, are unique to PLATO IV type situations.

- [105] See Bigelow, Computer Law Service, Introduction to art 3, § 3.
- [106] See Saragovitz, "Patents - Trade Secrets - Technical Data Use and Misuse by the U.S. Government," 15 Vill. L.Rev. 331 (1970).
- [107] Wofsey, "Contracting For Software," Computer Law Service art. 2, § 3-3 (ed by Bigelow).
- [108] See Levy, "Computer Programs in Government Procurement," 10 Will. and Mary L. R. 658 (1969). See also C.C.H. Gov't. Contracts Rep. IP 14,110; 14,200; 14,205; 14,220.
- [109] N.A.S.A. IP 9.101-4.
- [110] Under A.S.P.R. § 9-201, unlimited rights in data means that the Federal Government has the right to use, duplicate, or disclose technical data in any manner and for any purpose.
- [111] 49 Opinions of the Comptroller General 124, 2 Comp. Law Serv. Rep. 291 (1969).
- [112] Proposed A.S.P.R. Change to Amend 9-202-2(c) (Case 70-83) discussed in 178 B.N.A. Patent, Trademark, and Copyright Rep. A-18 (May 16, 1974).
- [113] See Hinrichs, "Proprietary Data and Trade Secrets Under Department of Defense Contracts," 36 Mil. L.Rev. 61 (1967) (hereinafter Hinrichs).
- [114] 28 U.S.C. § 1494 (1970).
- [115] _____ F. Supp. _____, (Dist. Ct. 1973) 490 B.N.A. Fed Contract Rep. D-1 (July 23, 1973).
- [116] Hinrichs, 89.
- [117] See "Unauthorized Use of Proprietary Information by the Government: A Mixed Bag of Remedies," 512 B.N.A. Fed. Contract Rep. K-1 (July 1, 1974).
- [118] See Kostos, "Unauthorized Use of Technical Data in Government Contracts: Remedies of the Data Owner," 6 Boston Coll. Ind. and Com. L.R. 753 (1965)



UNIVERSITY OF ILLINOIS-URBANA

510.841L63C

C001

CAC DOCUMENTS\$URBANA

111-120 1974



3 0112 007263814